

Supply Chain Risk Management Standard

Date Issued: 06/11/2026

Revised Date: 06/11/2026

Authority: Chief Information Security Officer

Standard Statement

The Supply Chain Risk Management standard outlines the requirements necessary to achieve compliance with the Supply Chain Risk Management Policy.

This standard is based on the National Institute of Standards and Technologies (NIST) SP 800-53, Security and Privacy Controls, specifically the Supply Chain Risk Management Control Family.

Applicability of controls and control enhancements are applied utilizing the NIST SP 800-53B Control Baselines, Table 3-20. Security control baselines have an applicability based on level of impact (low-impact, moderate-impact, high-impact) derived from NIST SP800-60 Guide for Mapping of Information and Information System to Security Categories.

The control number “SR” identified on each control or control enhancement represents the NIST control number within the NIST SP 800-53 Supply Chain Risk Management Control Family.

Reason for the Standard

This standard is designed to address risks that can arise from vendors, contractors, and/or suppliers and ensure that MNIT proactively manages risks that could disrupt operations or compromise data security.

Applicability

This standard applies to all departments, agencies, offices, councils, boards, commissions, and other entities in the executive branch of Minnesota State Government. This document also applies to all vendors and contractors providing goods and services to these State entities.

Controls

Table 1: Supply Chain Risk Management Controls

Control Number	Control Name	Control Detail	Applicable Data Protection Categorization
SR-2	Supply Chain Risk Management Plan	1. Develop a Supply Chain Risk Management (SCRM) plan for managing supply chain risks associated with acquisition, delivery, integration, operations and maintenance, and disposal of systems, system components and/or system services: Agency-defined systems, system components, or systems services. 2. The SCRM Team must review and update the SCRM plan on an annual basis or as required, to address threat, organizational, and/or environmental changes. 3. The SCRM plan must be protected from unauthorized disclosure and modification.	Low Moderate High
SR-2(1)	Establish SCRM Team	Establish a Supply Chain Risk Management (SCRM) Team consisting of personnel with diverse roles to lead and support the SCRM activities including CISO or CISO designee(s), information technology, contracting, privacy, legal, acquisition, business continuity, and other relevant functions.	Low Moderate High
SR-3	Supply Chain Controls and Processes	1. Establish a process(es) to identify and address weaknesses or deficiencies in the supply chain element and processes of SCRM Team-defined system(s) and/or system components 2. Employ controls to protect against supply chain risks to the system, system component, or system service to limit the harm or consequences from supply chain-related events. 3. Document the selected and implemented supply chain processes and controls within system security plans, assessments, SCRM plan, agency-defined documents.	Low Moderate High

Control Number	Control Name	Control Detail	Applicable Data Protection Categorization
SR-3(2)	Limitation of Harm	Employ one or more of the following controls to limit harm from potential adversaries identifying and targeting the organizational supply chain: agency-defined controls. 1. Avoid purchase of custom or non-standardized configurations. 2. Employ approved vendor lists with standing reputations in industry. 3. Follow pre-agreed maintenance schedules update and patch delivery mechanisms. 4. Maintain a contingency plan in case of supply chain event. 5. Utilize procurement carve-outs that provide exclusions to commitments or obligations. 6. Use diverse delivery routes. 7. Minimize the time between purchase decisions and delivery.	High
SR-3(3)	Sub-Tier Flow Down	Ensure that the controls included in the contracts of prime contractors are also included in the contracts of subcontractors	High
SR-5	Acquisition Strategies, Tools, and Methods	Employ SCRM Team-defined acquisition strategies, contract tools, and procurement methods to protect against, identify, and mitigate supply chain risks.	Low Moderate High
SR-5(2)	Assessments Prior to Selection, Acceptance, Modification, or Update	Assess the system, system component, or system service prior to selection, acceptance, modification, or update.	High
SR-6	Supplier Assessments and Reviews	Assess and review annually the supply chain-related risks associated with vendors, suppliers, and/or contractors and the system, system component, or system service they provide.	Moderate High

Control Number	Control Name	Control Detail	Applicable Data Protection Categorization
SR-6(1)	Testing and Analysis	Employ one or more: organizational analysis, independent third-party analysis, organizational testing, independent third-party testing of supply chain elements processes, and/or actors associated with the system, system component, and/or system service.	High
SR-8	Notification Agreements	Establish agreements and procedures with entities involved in the supply chain for the system, system component, or system service for the (one or more): 1. Notification of supply chain compromises 2. Agency-defined results of assessments or audits	Low Moderate High
SR-9	Tamper Resistance and Detection	Implement a tamper protection program for the system, system component, or system service.	High
SR-9(1)	Multiple Stages of System Development Lifecycle	Employ anti-tamper technologies, tools, and techniques throughout the system development life cycle.	High
SR-10	Inspection of Systems and/or Components	Inspect Agency-defined systems or system components [Selection (one or more): at random; at an Agency-defined frequency, upon Agency-defined indications of need for inspection] to detect tampering.	Low Moderate High
SR-11	Component Authenticity	1. Develop and implement anti-counterfeit policy and procedures that include the means to detect and prevent counterfeit components from entering the system; and 2. Report counterfeit system components to (one or more): a. SCRM team-defined external reporting agencies b. Source of counterfeit component	Low Moderate High

Control Number	Control Name	Control Detail	Applicable Data Protection Categorization
SR-11(1)	Anti-Counterfeit Training	Train SCRM team-defined personnel or roles to detect counterfeit system components (including hardware, software, and firmware).	Low Moderate High
SR-11(2)	Anti-Counterfeit Scanning	Maintain configuration control over the following system components awaiting service or repair and serviced or repaired components awaiting return to service: SCRM team-defined system components.	Low Moderate High
SR-12	Component Disposal	Dispose of Agency-defined data, documentation, tools, and/or system components using SCRM defined media sanitization and disposal techniques and methods	Low Moderate High

Roles & Responsibilities

- Employees, Vendors, and Contractors are responsible for:
 - 1.1. Reading, understanding, and applying relevant supply chain risk management policies, standards, and procedures.
 - 1.2. Ensure supply chain risk management is incorporated into vendor solicitation, project planning, procurement, system integration, and vendor management processes prior to submitting a requisition request.
 - 1.3. Ensure that vendors and contractors follow required supply chain risk management controls.
 - 1.4. Contact appropriate management personnel with questions about supply chain risk management policies, standards, or procedures.
- Supervisors and Managers are responsible for:
 - 2.1. Ensure employees and contractors are proficient in supply chain risk management policies, standards, and procedures that are relevant to their roles.
 - 2.2. Ensuring that the standard is implemented and enforced for all third-party engagements.
 - 2.3. Hold employees accountable for following supply chain risk management policies and procedures.
 - 2.4. Ensuring that KPIs are measured, monitored, and reported to the CISO on a quarterly/annual basis.

3. Project Managers, Product Owners, and Business Analysts are responsible for:
 - 3.1. Ensure all project scoping and project work complies with all MNIT policies, standards, and guidelines.
 - 3.2. Ensure that risk assessments are completed for all supply chain suppliers and service providers before procurement, focusing on cybersecurity, operational, and regulatory risks.
 - 3.3. Where feasible, ensure an approved list of alternate suppliers and service providers in case of failure or disruption from a key supplier.
 - 3.4. In partnership with Security personnel, conduct additional due diligence on suppliers, including evaluating their financial stability, security posture, and ability to meet organizational requirements.
 - 3.5. Communicate to procurement when a potential purchase may be in scope for supply chain risk management
4. Procurement Personnel are responsible for:
 - 4.1. Incorporate standards in procurement processes to satisfy in-scope requirements of this document.
 - 4.2. Work with in-scope vendors and suppliers to include MNIT template language in contract documents.
 - 4.3. Establish notification agreements with in-scope suppliers requiring timely disclosure of supply-chain incidents, breaches, or material changes affecting component integrity or provenance.
5. Information Technology Personnel are responsible for:
 - 5.1. Apply appropriate supply chain risk controls during the design, operation, and maintenance of systems and services.
 - 5.2. Work with third parties to ensure security controls are implemented for critical systems and components.
6. Information Security Personnel are responsible for:
 - 6.1. Ensure supply chain security requirements are aligned with supply chain risk management and organizational security policies.
 - 6.2. Monitor supply chain risks and respond to any security breaches or incidents within the supply chain.
 - 6.3. Coordinate supply chain notifications and determine escalation and public disclosure in coordination with Legal.
 - 6.4. Review and update supply chain risk management solicitation and contract language as needed
7. Governance, Risk, and Compliance Personnel are responsible for:
 - 7.1. Develop, maintain, and assess compliance with supply chain risk management requirements.
 - 7.2. Provide training on supply chain risk management policies, standards, and procedures.
 - 7.3. Assist with the interpretation and application of supply chain risk management policies.
8. State Chief Information Security Officer (CISO) and/or designee is accountable for:
 - 8.1. Review and approve this standard.

Related Information

National Institute for Standards and Technologies (NIST) SP800-53A, Rev 5

National Institute for Standards and Technologies (NIST) SP800-53B, Rev 5

Secure Systems Development and Acquisition Standard

Supply Chain Risk Management Policy

Threat and Vulnerability Management Standard

Definitions

Table 2 – Definitions

Term	Definition
Agency-defined	Agency-stated parameters.
Supply chain	Linked set of resources and processes between and among multiple levels of organizations, each of which is an acquirer, that begins with the sourcing of products and services and extends through their life cycle.

History

Table 3 – Version History

Version	Description	Date
1.0	Initial version reviewed and approved executive leadership	6/11/2026

Contact

grc@state.mn.us